PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-244584
(43)Date of publication of application : 19.09.1995

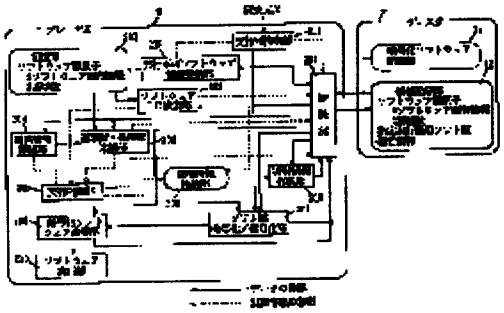
(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 06-032601
(22)Date of filing : 02.03.1994

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : OMORI MOTOJI
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO
MIYAJI MITSUKO

(54) SOFTWARE PROTECTION SYSTEM

(57)Abstract:
PURPOSE: To attain execution by an optional execution device by a procedure for changing a specified execution device in a software protection system which can not be executed by an execution device other than the specified one.



CONSTITUTION: Whether a software identifier(ID) recorded in an information recording part 12 of a disk 1 is stored in a storage part 203 or not is retrieved. When the corresponding ID is stored in the storage part 203, the accumulated number of IDs is compared with a reference number stored in the storage part 203, and only when the accumulated number is larger, the execution of the software is permitted. Also when the corresponding ID is not stored in the storage part 203, the execution of the software is permitted. In this case, a software key in the recording part 12 is decoded by a software key ciphering/ decoding part 207, ciphered software recorded in a ciphered software recording part 11 is decoded by using the software key and executed by a software execution part 210. At the time of changing a specified execution device, the accumulated number of IDs and the reference value are changed and a software key is rewritten to a key for a changed execution device.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平7－244584

(43)公開日　平成７年(1995)９月19日

(51)Int.Cl.⁶		識別記号	庁内整理番号	FI	技術表示箇所
G06F	9/06	550	H 7230－5B		
			C 7230－5B		
			L 7230－5B		
	12/14	320	F		

審査請求　未請求　請求項の数８　ＯＬ　（全 18 頁）

(21)出願番号　特願平6－32601

(22)出願日　平成６年(1994)３月２日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　小笠原　史朗

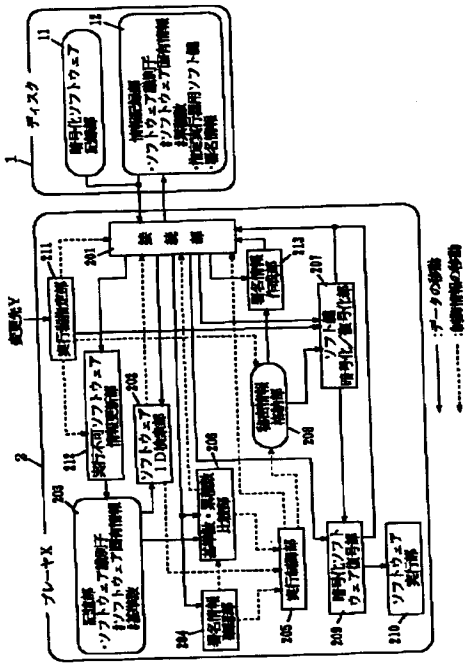
最終頁に続く

(54)【発明の名称】　ソフトウェア保護システム

(57)【要約】　（修正有）

【目的】　指定実行器以外では実行できないようなソフトウェア保護システムにおいて、指定実行器の変更手続きにより任意の実行器での実行を可能にする。

【構成】　ディスク１の情報記録部１２に記録されているソフトウェア識別子が、記憶部２０３にあるかどうか検索する。該当識別子が記憶部２０３にあった場合は、ソフトウェア識別子の累積数と記憶部に記憶されている基準数の大小関係が比較され、累積数のほうが大なるときのみソフトウェアの実行が許可される。また該当識別子が記憶部２０３にない場合もソフトウェアの実行が許可される。その場合は、情報記録部１２のソフト鍵がソフト鍵暗号化／復号化部２０７で復号され、ソフト鍵を用いて、暗号化ソフトウェア記録部１１に記録されている暗号化ソフトウェアを復号化し、ソフトウェア実行部２１０で実行する。指定実行器の変更では、識別子の累積数、基準数が変更され、ソフト鍵が変更先の実行器用に書き換えられる。



1

【特許請求の範囲】

【請求項１】　記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、

前記記録媒体には、

ソフトウェアと、

前記ソフトウェアまたは前記記録媒体に固有の第１の固有情報と、

前記ソフトウェアを実行させるべき実行器に固有の第２の固有情報とが格納されており、

前記実行器は、

前記記録媒体から前記ソフトウェアおよび前記第２の固有情報を読み出し、当該第２の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるチェック手段、

前記ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、

前記記録媒体に格納された第２の固有情報を、前記実行器指定手段で指定された他の実行器に固有の情報に変換する変換手段、

実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、

前記実行器指定手段によって実行器の変更先が指定されたとき、前記記録媒体に格納された第１の固有情報を、前記実行不可情報記憶手段に書き込む固有情報書き込み手段、および前記記録媒体に格納されている第１の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けないように前記チェック手段を制御する第１の実行制御手段を備える、ソフトウェア保護システム。

【請求項２】　前記記録媒体には、さらに、前記第１の固有情報と対にして累積数が格納されており、

前記実行不可情報記憶手段には、さらに、前記第１の固有情報と対にして基準数が記憶されており、

前記累積数および前記基準数は、初期値が同一値に選ばれており、

前記実行器は、前記実行器指定手段によって実行器の変更先が指定されたとき、前記累積数および前記基準数のそれぞれに所定値を加算する加算手段をさらに備え、

前記第１の実行制御手段は、

前記記録媒体に格納されている第１の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されていない場合、または前記記録媒体に格納されている第１の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されているが前記累積数が前記基準数よりも大きい場合は、当該記録媒体に格納されているソフトウェアの実行許可を前記チェック手段に与え、

前記記録媒体に格納されている第１の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されており、かつ前記累積数が前記基準数と等しいかまたはそれよりも小さい場合は、当該記録媒体に格納されているソフトウェアの実行不許可を前記チェック手段に与えることを特徴とする、請求項１に記載のソフトウェア保護システム。

2

【請求項３】　前記記録媒体には、さらに、前記第１の固有情報と対にして乱数が格納されており、

前記実行不可情報記憶手段には、さらに、前記第１の固有情報と対にして乱数が記憶されており、

前記実行器は、さらに前記実行器指定手段によって実行器の変更先が指定されたとき、乱数を発生する乱数発生手段、

前記乱数発生手段によって乱数が発生される毎に、当該乱数を前記実行不可情報記憶手段に追加して書き込む乱数書き込み手段、および前記乱数発生手段によって乱数が発生される毎に、前記記録媒体に格納された乱数を書き換える乱数書き換え手段を備え、

前記第１の実行制御手段は、

前記記録媒体に格納されている第１の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されていない場合、または前記記録媒体に格納されている第１の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されているが前記記録媒体に格納されている乱数と同一の乱数が前記実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行許可を前記チェック手段に与え、

前記記録媒体に格納されている第１の固有情報と同一の固有情報が前記実行不可情報記憶手段に記憶されており、かつ前記記録媒体に格納されている乱数と同一の乱数が前記実行不可情報記憶手段に記憶されている場合は、当該記録媒体に格納されているソフトウェアの実行不許可を前記チェック手段に与えることを特徴とする、請求項１に記載のソフトウェア保護システム。

【請求項４】　前記記録媒体に格納されたソフトウェアは、暗号化されており、

前記記録媒体に格納された第２の固有情報は、暗号化されたソフト鍵であり、

前記チェック手段は、

実行器毎に異なる秘密情報を記憶する秘密情報記憶手段と、

前記記録媒体から前記ソフト鍵を読み出し、前記秘密情報を用いて復号化するソフト鍵復号化手段と、

前記記録媒体から前記暗号化されたソフトウェアを読み出し、前記復号化されたソフト鍵を用いて復号化するソフトウェア復号化手段と、

前記復号化されたソフトウェアを実行するソフトウェア実行手段とを含み、

前記変換手段は、

前記復号化されたソフト鍵を、前記実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能な

ように暗号化するソフト鍵暗号化手段と、
前記記録媒体に格納された暗号化されたソフト鍵を、前記ソフト鍵暗号化手段によって暗号化されたソフト鍵に書き換えるソフト鍵書き換え手段とを含む、請求項１～３のいずれかに記載のソフトウェア保護システム。
【請求項５】　前記記録媒体には、さらに、前記暗号化されたソフトウェア，前記第１の固有情報，前記暗号化されたソフト鍵および前記累積数の内、少なくともいずれか１つを対象として作成されたディジタル署名情報が格納されており、
前記実行器は、さらに前記記録媒体に格納されているディジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けないように前記チェック手段を制御する第２の実行制御手段、
前記実行器指定手段によって実行器の変更先が指定されたとき、前記秘密情報を用いて、前記ディジタル署名情報を作成するディジタル署名情報作成手段、および前記記録媒体に格納されたディジタル署名情報を、前記ディジタル署名情報作成手段によって作成されたディジタル署名情報に書き換える署名情報書き換え手段を備える、請求項４に記載のソフトウェア保護システム。
【請求項６】　前記記録媒体には、さらに、コピー可能回数が格納されており、
前記実行器は、さらに前記記録媒体をコピーした回数を示す累計数を記憶する累計数記憶手段、
前記記録媒体に格納されたコピー可能回数が前記累計数記憶手段に記憶された累計数よりも大きい場合のみ、当該記録媒体のコピーを実行するコピー制御手段、および前記コピー制御手段が前記記録媒体のコピーを実行する毎に、前記累計数記憶手段に記憶された累計数を更新する累計数更新手段を備える、請求項１～５のいずれかに記載のソフトウェア保護システム。
【請求項７】　ソフトウェアが格納された記録媒体を貸与する場合、貸し主側の実行器で変更手続きを行うことにより、当該ソフトウェアの実行が可能な借り主側の実行器を特定するようなソフトウェア保護システムであって、
前記記録媒体には、
暗号化されたソフトウェアと、
前記ソフトウェアまたは前記記録媒体に固有のソフトウェア／記録媒体固有情報と、
前記貸し主側の実行器に固有の暗号化された第１のソフト鍵と、
前記借り主側の実行器に固有の暗号化された第２のソフト鍵とが格納されており、
前記貸し主側の実行器は、
当該貸し主側の実行器に固有の第１の秘密情報を記憶する第１の秘密情報記憶手段、
前記記録媒体から前記第１のソフト鍵を読み出し、前記

第１の秘密情報を用いて復号化する第１のソフト鍵復号化手段、
前記記録媒体から前記暗号化されたソフトウェアを読み出し、前記復号化された第１のソフト鍵を用いて復号化する第１のソフトウェア復号化手段、
前記復号化されたソフトウェアを実行する第１のソフトウェア実行手段、
前記ソフトウェアを実行する前記借り主側の実行器を指定する実行器指定手段、
前記復号化された第１のソフト鍵を、前記実行器指定手段で指定された借り主側の実行器でのみ復号可能な第２のソフト鍵に暗号化するソフト鍵暗号化手段、および前記記録媒体に格納された暗号化された第２のソフト鍵を、前記ソフト鍵暗号化手段によって暗号化された第２のソフト鍵に書き換えるソフト鍵書き換え手段を備え、
前記借り主側の実行器は、
当該借り主側の実行器に固有の第２の秘密情報を記憶する第２の秘密情報記憶手段、
前記記録媒体から前記第２のソフト鍵を読み出し、前記第２の秘密情報を用いて復号化する第２のソフト鍵復号化手段、
前記記録媒体から前記暗号化されたソフトウェアを読み出し、前記復号化された第２のソフト鍵を用いて復号化する第２のソフトウェア復号化手段、
前記復号化されたソフトウェアを実行する第２のソフトウェア実行手段、
前記記録媒体の返却手続きを指示する返却手続き指示手段、
実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、
前記返却手続き指示手段によって返却手続きが指示されたとき、前記記録媒体に格納されたソフトウェア／記録媒体固有情報を、前記実行不可情報記憶手段に書き込む固有情報書き込み手段、および前記記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が前記実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けないように前記第２のソフトウェア実行手段を制御する実行制御手段を備える、ソフトウェア保護システム。
【請求項８】　記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、
前記記録媒体には、
暗号化されたソフトウェアと、
前記ソフトウェアまたは前記記録媒体に固有のソフトウェア／記録媒体固有情報とが格納されており、
前記実行器は、
実行器毎に異なる秘密情報を記憶する秘密情報記憶手段、

前記記録媒体から暗号化されたソフトウェアを読み出し、前記秘密情報を用いて復号化するソフトウェア復号化手段、
前記復号化されたソフトウェアを実行するソフトウェア実行手段、
前記ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、
前記復号化されたソフトウェアを、前記実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能なように暗号化するソフトウェア暗号化手段、
前記記録媒体に格納された暗号化されたソフトウェアを、前記ソフトウェア暗号化手段によって暗号化されたソフトウェアに書き換えるソフトウェア書き換え手段、
実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、
前記実行器指定手段によって実行器の変更先が指定されたとき、前記記録媒体に格納されたソフトウェア／記録媒体固有情報を、前記実行不可情報記憶手段に書き込む固有情報書き込み手段、および前記記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が前記実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けないように前記ソフトウェア実行手段を制御する実行制御手段を備える、ソフトウェア保護システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はソフトウェア保護システムに関し、より特定的には、記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムに関する。

【０００２】

【従来の技術】近年、種々のマルチメディア機器が開発され、ゲームや教育用のソフトウェアを始めとする多くの有償マルチメディアソフトウェアが販売されている。ところが、そのソフトウェアの保護は不完全であり、不正にコピーされたソフトウェアが数多く出回っているのが現状である。このような不正なコピーを防ぐために特許法や著作権法等の法律の規制があるが、同時にメカニズム面からのソフトウェア保護も必要である。

【０００３】例えば、ソフトウェアを格納する記録媒体（フロッピーディスク等）のフォーマットを特殊なものにすることによって、ＯＳ（オペレーティング・システム）で提供されているコピー機能では複製ができないようにする方法がある。しかしながら、このような方法でもビットごとにコピーを行なうタイプのコピーツールを用いれば、多くの場合複製が可能である。また、正規のユーザにとっては、バックアップディスクが作れないといった不都合も生じる。

【０００４】また、ソフトウェアを暗号化してコピー防止を行なう方法が提案されている。この方法は、例えば特開昭６１－１４５６４２号公報に示されている。図７にその構成を示す。図７において、パーソナルコンピュータ５０１は、暗号機構５０２を含む。ソフトウェア販売業者によって販売されるプログラム５０３は、一意的なファイルキーＫＦで暗号化されており、１つのプログラムファイルとしてディスク（特開昭６１－１４５６４２号公報では、ディスケットと称している）上に書き込まれている。

【０００５】暗号化されたプログラム５０３が格納されたディスクを購入するユーザーは、まずソフトウェア販売業者からキー配送センタ５０４で生成される秘密のパスワードを取得しなければならない。このパスワードにより、暗号化されたプログラム５０３は、適切に初期設定された暗号機構５０２を有する予め指定されたパーソナルコンピュータ５０１だけで解読し実行することができる。この秘密のパスワードは、特定のプログラムおよびこれが復元され実行される特定のコンピュータに対して一意的なものである。このパスワードによれば、他の暗号化されたプログラムをそのコンピュータで復元することはできず、同じ暗号化されたプログラムを他のコンピュータで復元することもできない。また、暗号化されたプログラムが格納されたディスクをコピーしても、予め指定されたパーソナルコンピュータ以外のコンピュータでは復元することはできず、コピーしても意味がなくなる。これによりコピー防止機能が実現されている。

【０００６】

【発明が解決しようとする課題】しかしながら、上記従来のソフトウェア保護方式では、正当なソフトウェアの持ち主であっても、ソフトウェアを予め指定された実行器以外では実行できないため、ソフトウェアを他の場所で実行することや、他のユーザにソフトウェアを譲渡することが困難である。

【０００７】他の場所での実行を可能にするためには、ソフトウェアを格納した記録媒体だけでなく、予め指定されたパーソナルコンピュータ５０１も移動することが考えられるが、パーソナルコンピュータ５０１が一般には記録媒体に比べて大型で移動しにくいことを考慮すると非現実的である。

【０００８】一方、ソフトウェアの譲渡を有効にするためには、パーソナルコンピュータ５０１ごとソフトウェアを他のユーザに譲ることが考えられるが、これもパーソナルコンピュータ５０１がもともとそのユーザに所属するものであり、複数のソフトウェアを実行するものであることを考慮すると、１つのソフトウェアを他のユーザに譲るために本体ごと譲るというのもまた非現実的である。この場合、ユーザ側で譲渡先のユーザ用のソフトウェアを作成することも考えられるが、元のソフトウェアが譲渡元でも実行可能であるため、実質的な譲渡が成立しない。

【０００９】それゆえに、本発明の目的は、ソフトウェアを他の実行器でも実行でき、かつ不法なコピーも防止し得るソフトウェア保護システムを提供することである。本発明の他の目的は、ソフトウェアを貸与する場合に好適するソフトウェア保護システムを提供することである。本発明のさらに他の目的は、ソフトウェアのコピー回数を制御できるソフトウェア保護システムを提供することである。

【００１０】

【課題を解決するための手段】請求項１に係る発明は、記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、記録媒体には、ソフトウェアと、ソフトウェアまたは記録媒体に固有の第１の固有情報と、ソフトウェアを実行させるべき実行器に固有の第２の固有情報とが格納されており、実行器は、記録媒体からソフトウェアおよび第２の固有情報を読み出し、当該第２の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるチェック手段、ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、記録媒体に格納された第２の固有情報を、実行器指定手段で指定された他の実行器に固有の情報に変換する変換手段、実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、実行器指定手段によって実行器の変更先が指定されたとき、記録媒体に格納された第１の固有情報を、実行不可情報記憶手段に書き込む固有情報書き込み手段、および記録媒体に格納されている第１の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにチェック手段を制御する第１の実行制御手段を備えている。

【００１１】請求項２に係る発明は、請求項１の発明において、記録媒体には、さらに、第１の固有情報と対にして累積数が格納されており、実行不可情報記憶手段には、さらに、第１の固有情報と対にして基準数が記憶されており、累積数および基準数は、初期値が同一値に選ばれており、実行器は、実行器指定手段によって実行器の変更先が指定されたとき、累積数および基準数のそれぞれに所定値を加算する加算手段をさらに備え、第１の実行制御手段は、記録媒体に格納されている第１の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されていない場合、または記録媒体に格納されている第１の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されているが累積数が基準数よりも大きい場合は、当該記録媒体に格納されているソフトウェアの実行許可をチェック手段に与え、記録媒体に格納されている第１の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されており、かつ累積数が基準数と等しいかまたはそれよりも小さい場合は、当該記録媒体に格納されているソフトウェアの実行不許可をチェック手段に与えることを特徴とする。

【００１２】請求項３に係る発明は、請求項１の発明において、記録媒体には、さらに、第１の固有情報と対にして乱数が格納されており、実行不可情報記憶手段には、さらに、第１の固有情報と対にして乱数が記憶されており、実行器は、さらに実行器指定手段によって実行器の変更先が指定されたとき、乱数を発生する乱数発生手段、乱数発生手段によって乱数が発生される毎に、当該乱数を実行不可情報記憶手段に追加して書き込む乱数書き込み手段、および乱数発生手段によって乱数が発生される毎に、記録媒体に格納された乱数を書き換える乱数書き換え手段を備え、第１の実行制御手段は、記録媒体に格納されている第１の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されていない場合、または記録媒体に格納されている第１の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されているが記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行許可をチェック手段に与え、記録媒体に格納されている第１の固有情報と同一の固有情報が実行不可情報記憶手段に記憶されており、かつ記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されている場合は、当該記録媒体に格納されているソフトウェアの実行不許可をチェック手段に与えることを特徴とする。

【００１３】請求項４の発明は、請求項１～３のいずれかの発明において、記録媒体に格納されたソフトウェアは、暗号化されており、記録媒体に格納された第２の固有情報は、暗号化されたソフト鍵であり、チェック手段は、実行器毎に異なる秘密情報を記憶する秘密情報記憶手段と、記録媒体からソフト鍵を読み出し、秘密情報を用いて復号化するソフト鍵復号化手段と、記録媒体から暗号化されたソフトウェアを読み出し、復号化されたソフト鍵を用いて復号化するソフトウェア復号化手段と、復号化されたソフトウェアを実行するソフトウェア実行手段とを含み、変換手段は、復号化されたソフト鍵を、実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能なように暗号化するソフト鍵暗号化手段と、記録媒体に格納された暗号化されたソフト鍵を、ソフト鍵暗号化手段によって暗号化されたソフト鍵に書き換えるソフト鍵書き換え手段とを含むことを特徴とする。

【００１４】請求項５に係る発明は、請求項４の発明において、記録媒体には、さらに、暗号化されたソフトウェア，第１の固有情報，暗号化されたソフト鍵および累積数の内、少なくともいずれか１つを対象として作成されたディジタル署名情報が格納されており、実行器は、さらに記録媒体に格納されているディジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けないよ

うにチェック手段を制御する第２の実行制御手段、実行器指定手段によって実行器の変更先が指定されたとき、秘密情報を用いて、ディジタル署名情報を作成するディジタル署名情報作成手段、および記録媒体に格納されたディジタル署名情報を、ディジタル署名情報作成手段によって作成されたディジタル署名情報に書き換える署名情報書き換え手段を備えている。

【００１５】請求項６に係る発明は、請求項１～５のいずれかの発明において、記録媒体には、さらに、コピー可能回数が格納されており、実行器は、さらに記録媒体をコピーした回数を示す累計数を記憶する累計数記憶手段、記録媒体に格納されたコピー可能回数が累計数記憶手段に記憶された累計数よりも大きい場合のみ、当該記録媒体のコピーを実行するコピー制御手段、およびコピー制御手段が記録媒体のコピーを実行する毎に、累計数記憶手段に記憶された累計数を更新する累計数更新手段を備えている。

【００１６】請求項７に係る発明は、ソフトウェアが格納された記録媒体を貸与する場合、貸し主側の実行器で変更手続きを行うことにより、当該ソフトウェアの実行が可能な借り主側の実行器を特定するようなソフトウェア保護システムであって、記録媒体には、暗号化されたソフトウェアと、ソフトウェアまたは記録媒体に固有のソフトウェア／記録媒体固有情報と、貸し主側の実行器に固有の暗号化された第１のソフト鍵と、借り主側の実行器に固有の暗号化された第２のソフト鍵とが格納されており、貸し主側の実行器は、当該貸し主側の実行器に固有の第１の秘密情報を記憶する第１の秘密情報記憶手段、記録媒体から第１のソフト鍵を読み出し、第１の秘密情報を用いて復号化する第１のソフト鍵復号化手段、記録媒体から暗号化されたソフトウェアを読み出し、復号化された第１のソフト鍵を用いて復号化する第１のソフトウェア復号化手段、復号化されたソフトウェアを実行する第１のソフトウェア実行手段、ソフトウェアを実行する借り主側の実行器を指定する実行器指定手段、復号化された第１のソフト鍵を、実行器指定手段で指定された借り主側の実行器でのみ復号可能な第２のソフト鍵に暗号化するソフト鍵暗号化手段、および記録媒体に格納された暗号化された第２のソフト鍵を、ソフト鍵暗号化手段によって暗号化された第２のソフト鍵に書き換えるソフト鍵書き換え手段を備え、借り主側の実行器は、当該借り主側の実行器に固有の第２の秘密情報を記憶する第２の秘密情報記憶手段、記録媒体から第２のソフト鍵を読み出し、第２の秘密情報を用いて復号化する第２のソフト鍵復号化手段、記録媒体から暗号化されたソフトウェアを読み出し、復号化された第２のソフト鍵を用いて復号化する第２のソフトウェア復号化手段、復号化されたソフトウェアを実行する第２のソフトウェア実行手段、記録媒体の返却手続きを指示する返却手続き指示手段、実行不可なソフトウェアに関する情報を記憶する

実行不可情報記憶手段、返却手続き指示手段によって返却手続きが指示されたとき、記録媒体に格納されたソフトウェア／記録媒体固有情報を、実行不可情報記憶手段に書き込む固有情報書き込み手段、および記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けないように第２のソフトウェア実行手段を制御する実行制御手段を備えている。

【００１７】請求項８に係る発明は、記録媒体に格納されたソフトウェアを、予め指定された実行器でのみ実行させるようなソフトウェア保護システムであって、記録媒体には、暗号化されたソフトウェアと、ソフトウェアまたは記録媒体に固有のソフトウェア／記録媒体固有情報とが格納されており、実行器は、実行器毎に異なる秘密情報を記憶する秘密情報記憶手段、記録媒体から暗号化されたソフトウェアを読み出し、秘密情報を用いて復号化するソフトウェア復号化手段、復号化されたソフトウェアを実行するソフトウェア実行手段、ソフトウェアを実行する実行器の変更先を指定する実行器指定手段、復号化されたソフトウェアを、実行器指定手段で指定された他の実行器における秘密情報でのみ復号可能なように暗号化するソフトウェア暗号化手段、記録媒体に格納された暗号化されたソフトウェアを、ソフトウェア暗号化手段によって暗号化されたソフトウェアに書き換えるソフトウェア書き換え手段、実行不可なソフトウェアに関する情報を記憶する実行不可情報記憶手段、実行器指定手段によって実行器の変更先が指定されたとき、記録媒体に格納されたソフトウェア／記録媒体固有情報を、実行不可情報記憶手段に書き込む固有情報書き込み手段、および記録媒体に格納されているソフトウェア／記録媒体固有情報と同一のソフトウェア／記録媒体固有情報が実行不可情報記憶手段に記憶されている場合、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにソフトウェア実行手段を制御する実行制御手段を備えている。

【００１８】

【作用】請求項１に係る発明においては、ソフトウェアを実行させるべき実行器に固有の第２の固有情報を記録媒体に格納しておき、実行器では、記録媒体からソフトウェアおよび第２の固有情報を読み出し、当該第２の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるようにしている。これによって、ソフトウェアを実行可能な実行器を予め特定することができる。また、ソフトウェアを実行する実行器の変更先が指定されると、記録媒体に格納された第２の固有情報を、指定された他の実行器に固有の情報に変換するようにしている。これによって、ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。

また、実行器の変更先が指定されると、記録媒体に格納された第１の固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されている第１の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしている。これによって、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【００１９】請求項２に係る発明においては、ソフトウェアを実行する実行器の変更先が指定されたとき、記録媒体に格納された累積数および実行不可情報記憶手段に記憶された基準数のそれぞれに所定値を加算するようにしている。その後、実行不可情報記憶手段に記憶されている第１の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、累積数が基準数よりも大きい場合のみ、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。これによって、変更先の実行器において再び元の実行器が変更先として指定された場合、元の実行器でのソフトウェアの実行が可能となる。

【００２０】請求項３に係る発明においては、ソフトウェアを実行する実行器の変更先が指定されたとき、実行器で乱数を発生し、この乱数を実行不可情報記憶手段に追加して書き込むと共に、記録媒体に格納された乱数を当該乱数で書き換えるようにしている。その後、実行不可情報記憶手段に記憶されている第１の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。これによって、変更先の実行器において再び元の実行器が変更先として指定された場合、元の実行器でのソフトウェアの実行が可能となる。

【００２１】請求項４に係る発明においては、暗号化されたソフト鍵を記録媒体に格納しておき、実行器では、このソフト鍵を固有の秘密情報を用いて復号化し、さらに復号化されたソフト鍵を用いて、記録媒体から読み出したソフトウェアを復号化し実行するようにしている。これによって、ソフトウェアを実行可能な実行器を予め特定することができる。また、ソフトウェアを実行する実行器の変更先が指定されると、復号化されたソフト鍵を、指定された他の実行器でのみ復号可能なように暗号化し、記録媒体に格納された暗号化されたソフト鍵を、このとき暗号化されたソフト鍵に書き換えるようにしている。これによって、ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納されたソフトウェア固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されている

ソフトウェア固有情報と同一のソフトウェア固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしている。これによって、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【００２２】請求項５に係る発明においては、暗号化されたソフトウェア，ソフトウェア固有情報，暗号化されたソフト鍵および累積数の内、少なくともいずれか１つを対象として作成されたディジタル署名情報を記録媒体に格納しておき、実行器では、記録媒体に格納されているディジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしている。これによって、記録媒体の格納情報の正当性をより正確に確認でき、不正な複製品を防止できる。

【００２３】請求項６に係る発明においては、記録媒体がコピーされる毎に更新される累計数を実行器に記憶しておき、記録媒体に格納されたコピー可能回数が当該累計数よりも大きい場合のみ、当該記録媒体のコピーを許可するようにしている。これによって、記録媒体のコピー回数を予め定められた回数に制限することができる。

【００２４】請求項７に係る発明においては、貸し主側の実行器は、記録媒体に格納された第１のソフト鍵を用いてソフトウェアの復号化を行う。したがって、借り主側の実行器では、記録媒体を貸し主に返却するとき、記録媒体中の第２のソフト鍵を書き換える必要がない。

【００２５】請求項８に係る発明においては、記録媒体に格納されたソフトウェア自体が、指定された実行器でのみ復号可能なように暗号化されている。したがって、実行器では、固有の秘密情報を用いて、ソフトウェアを復号化し実行する。

【００２６】

【実施例】

（１）第１の実施例

図１は、本発明の第１の実施例に係るソフトウェア保護システムの構成を示すブロック図である。なお、図１において、実線の矢印はデータの移動を示し、破線の矢印は制御情報の移動を示している。また、以下の説明において、ソフトウェアとは、例えばアプリケーションプログラムを意味するものとする。

【００２７】図１において、ディスク１は、暗号化ソフトウェア記録部１１と、情報記録部１２とを含む。暗号化ソフトウェア記録部１１には、暗号化ソフトウェアＥ（ＫＡ，ｓｏｆｔＡ）が格納されている。情報記録部１２には、ソフトウェアの種別を表すソフトウェア固有情報ＩＤＡおよびソフトウェアを実行できる指定実行器の変更回数を表す累積数ＣＮＴ［Ａ］を含むソフトウェア識別子と、指定された実行器でしか復号できない指定実行器用ソフト鍵Ｅ（Ｘ，ＫＡ）と、これら各情報の正当

性を示す署名情報とが記録されている。

【００２８】プレーヤ２は、ディスク１内のソフトウェア識別子，指定実行器用ソフト鍵Ｅ（Ｘ，ＫＡ）および署名情報の内容を確認してソフトウェアの実行を行ない、さらに指定実行器の変更手続きを行なう機能を有している。このプレーヤ２は、接続部２０１と、ソフトウェアＩＤ検索部２０２と、記憶部２０３と、署名情報確認部２０４と、実行制御部２０５と、基準数・累積数比較部２０６と、ソフト鍵暗号化／復号化部２０７と、秘密情報格納部２０８と、暗号化ソフトウェア復号部２０９と、ソフトウェア実行部２１０と、実行器指定部２１１と、実行不可ソフトウェア情報更新部２１２と、署名情報作成部２１３とを備えている。

【００２９】接続部２０１は、ディスク１をプレーヤ２に着脱自在に接続するもので、ディスク１から各情報を読み出し、ディスク１に所定の情報を書き込む機能を有している。ソフトウェアＩＤ検索部２０２は、入力されるソフトウェア固有情報ＩＤＡが、記憶部２０３に実行不可ソフトウェアとして記憶されているかどうかを検索する機能を有している。記憶部２０３は、実行不可ソフトウェアのソフトウェア固有情報ＩＤＡ’と、ソフトウェアを実行不可状態にしたときの情報記録部１２に記録されている累積数ＣＮＴ［Ａ］と同じ値である基準数ＮＵＭ［Ａ］を対にしてソフトウェア識別子として記憶している。

【００３０】署名情報確認部２０４は、記憶部２０３において実行不可ソフトウェアとして記録されているソフトウェアに対して、情報記録部１２に記録されている署名情報が正当なものかどうかを確認し、署名情報が正当な場合は基準数・累積数比較部２０６に基準数ＮＵＭ［Ａ］と累積数ＣＮＴ［Ａ］の比較を行うように指示し、署名情報が不当な場合は実行制御部２０５にそのソフトウェアの実行不許可の情報を入力する機能を有している。実行制御部２０５は、署名情報確認部２０４から入力される情報（情報記録部１２に記録された署名情報が正当か否かを示す情報）と、基準数・累積数比較部２０６から入力される情報（そのソフトウェアの実行許可・不許可の情報）とに基づいて、暗号化ソフトウェアＥ（ＫＡ，ｓｏｆｔＡ）を復号化するかどうかの制御を行なう機能を有している。基準数・累積数比較部２０６は、署名情報確認部２０４で署名情報が正当と確認されたディスク１に対して、記憶部２０３に記憶されている該ソフトウェアの基準数ＮＵＭ［Ａ］と情報記録部１２に記録されている累積数ＣＮＴ［Ａ］との大小関係を比較し、その結果に基づいてソフトウェアの実行許可・不許可の情報を実行制御部２０５に入力する機能を有している。

【００３１】ソフト鍵暗号化／復号化部２０７は、情報記録部１２に記録されている指定実行器用ソフト鍵Ｅ（Ｘ，ＫＡ）を、秘密情報格納部２０８に格納されているプレーヤ２に固有の秘密情報ＳＸで復号化し、また指定された実行器の変更がある場合は、変更先用の指定実行器用ソフト鍵に暗号化する機能を有している。秘密情報格納部２０８は、プレーヤ２に固有の秘密情報ＳＸを記録している。暗号化ソフトウェア復号部２０９は、暗号化ソフトウェア記録部１１に記録されている暗号化ソフトウェアＥ（ＫＡ，ｓｏｆｔＡ）が入力され、ソフト鍵暗号化／復号化部２０７で復号化されたソフト鍵で、暗号化ソフトウェアＥ（ＫＡ，ｓｏｆｔＡ）を復号化する機能を有している。ソフトウェア実行部２１０は、暗号化ソフトウェア復号部２０９で復号化されたソフトウェアｓｏｆｔＡを実行する機能を有している。

【００３２】実行器指定部２１１は、入力された変更先情報に従って指定先実行器用ソフト鍵の変更をソフト鍵暗号化／復号化部２０７で行うように制御し、情報記録部１２に記録されている累積数ＣＮＴ［Ａ］の書き換えを行うように接続部２０１に指示し、それに伴い記憶部２０３に記憶されている情報の変更を実行不可ソフトウェア情報更新部２１２に指示し、新しいソフトウェア識別子に対する署名情報の作成を署名情報作成部２１３に指示する機能を有している。実行不可ソフトウェア情報更新部２１２は、指定実行器の変更のときに、情報記録部１２に記録されている累積数の書き換えを行うのに伴い、記憶部２０３に記憶されている情報の変更を行なう機能を有している。署名情報作成部２１３は、実行不可ソフトウェア情報更新部２１２によって変更された新しいソフトウェア識別子に対する署名情報の作成を行なう機能を有している。

【００３３】なお、図１のプレーヤ２内において、ソフトウェアＩＤ検索部２０２、記憶部２０３、署名情報確認部２０４、実行制御部２０５、基準数・累積数比較部２０６、ソフト鍵暗号化／復号化部２０７、秘密情報格納部２０８、暗号化ソフトウェア復号部２０９、ソフトウェア実行部２１０、実行器指定部２１１、実行不可ソフトウェア情報更新部２１２および署名情報作成部２１３は、それぞれ変更，解析，複製できない領域に配置されている。

【００３４】概説すると、上記第１の実施例のソフトウェア保護システムは、ソフトウェアｓｏｆｔＡ自体はそのソフトウェアの全ディスク共通の鍵ソフト鍵ＫＡで暗号化し、そのソフト鍵ＫＡをその指定された実行器であるプレーヤ２でしか復号できないように暗号化することによって、指定された実行器以外では実行できないことを実現している。

【００３５】図２は、上記第１の実施例のソフトウェア保護システムにおけるソフトウェア実行動作の処理手順を示すフローチャートである。また、図３は、上記第１の実施例のソフトウェア保護システムにおける指定実行器の変更手続きの処理手順を示すフローチャートである。以下、これら図２および図３を参照して、上記第１

の実施例の動作を説明する。

【００３６】なお、以下では、図１のプレーヤ２（以下、プレーヤＸと表現する）用として暗号化されたソフト鍵Ｅ（Ｘ，ＫＡ）を持つ暗号化ソフトウェアＥ（ＫＡ，ｓｏｆｔＡ）が復号化されて実行され、その後、図示しない他のプレーヤ（以下、プレーヤＹと表現する）用に指定プレーヤの変更手続きを行なう場合の動作について説明する。また、以下の説明において、ソフト鍵Ｅ（Ｘ，ＫＡ）は、ソフト鍵ＫＡをプレーヤＸに固有の秘密情報ＳＸでのみ復号化される形式で暗号化したものを示している。また、ソフトウェアＥ（ＫＡ，ｓｏｆｔＡ）は、ソフトウェアｓｏｆｔＡをソフト鍵ＫＡで暗号化したものを示し、ソフト鍵ＫＡで復号化される。

【００３７】（ａ）暗号化ソフトウェアの復号・実行動作

最初に、図２を参照して、暗号化ソフトウェアの復号・実行動作を説明する。まず、接続部２０１にディスク１が接続される（ステップＳ１０１）。次に、情報記録部１２に記録されているソフトウェア識別子のソフトウェア固有情報ＩＤＡが、接続部２０１を通してソフトウェアＩＤ検索部２０２に入力される。ソフトウェアＩＤ検索部２０２は、当該入力されたソフトウェア固有情報ＩＤＡと一致する実行不可ソフトウェア固有情報ＩＤＡ'が、記憶部２０３に記憶されているかどうかを検索する（ステップＳ１０２）。

【００３８】上記ステップＳ１０２における検索の結果、入力されたソフトウェア固有情報ＩＤＡと一致する実行不可ソフトウェア固有情報ＩＤＡ'が記憶部２０３に記憶されている場合、ソフトウェアＩＤ検索部２０２は、接続部２０１を介して、情報記録部１２から署名情報とソフトウェア識別子とを読み出し、署名情報確認部２０４に入力する。署名情報確認部２０４は、情報記録部１２に記録されているソフトウェア識別子の内容が正当なものであるかどうかを、署名情報のディジタル署名作成者の実行器識別子（図示していないが、ディスク１内に格納されている）から容易に導かれるディジタル署名作成者の公開鍵で確認する（ステップＳ１０３）。ステップＳ１０３での確認の結果、ソフトウェア識別子が正当なものでないと判断した場合、署名情報確認部２０４は、実行制御部２０５にそのソフトウェアの実行を不許可とするように指示する（ステップＳ１０４）。従って、実行制御部２０５は、ソフトウェアの実行を行わない。

【００３９】一方、上記ステップＳ１０３における確認の結果、ソフトウェア識別子の内容が正当なものであると判断した場合、署名情報確認部２０４は、基準数・累積数比較部２０６に対して、記憶部２０３にソフトウェア識別子として実行不可ソフトウェア固有情報ＩＤＡ'と対に記憶されている基準数ＮＵＭ［Ａ］を、情報記録部１２内に記録されているソフトウェア識別子の累積数ＣＮＴ［Ａ］と比較するように指示する。応じて、基準数・累積数比較部２０６は、記憶部２０３からソフトウェア識別子として実行不可ソフトウェア固有情報ＩＤＡ'と対で記録されている基準数ＮＵＭ［Ａ］を読み出す。また、接続部２０１を介して、情報記録部１２に記録されているソフトウェア識別子の累積数ＣＮＴ［Ａ］を読み出す。次に、基準数・累積数比較部２０６は、入力された基準数ＮＵＭ［Ａ］と累積数ＣＮＴ［Ａ］とを比較する（ステップＳ１０５）。

【００４０】ディスク１に格納されたソフトウェアが正当なソフトウェアである場合は、後述の指定プレーヤ変更手続きにより、不等式ＮＵＭ［Ａ］＜ＣＮＴ［Ａ］が成り立ち、基準数・累積数比較部２０６は、実行制御部２０５にソフトウェアの実行許可情報を入力する（ステップＳ１０６）。一方、不等式ＮＵＭ［Ａ］＜ＣＮＴ［Ａ］が成り立たない場合は、ディスク１は指定実行器変更手続きによりすでに無効になったディスクであるので、実行制御部２０５にそのソフトウェアｓｏｆｔＡの実行不許可の情報を入力する（ステップＳ１０４）。したがって、この場合、実行制御部２０５は、ソフトウェアｓｏｆｔＡの実行を行わない。

【００４１】基準数・累積数比較部２０６からソフトウェアの実行許可が出た場合、実行制御部２０５は、接続部２０１を介して、情報記録部１２から指定実行器用ソフト鍵Ｅ（Ｘ，ＫＡ）を読み出し、ソフト鍵暗号化／復号化部２０７に入力する。また、実行制御部２０５は、秘密情報格納部２０８からプレーヤＸに固有の秘密情報ＳＸを読み出して、ソフト鍵暗号化／復号化部２０７に入力する。応じて、ソフト鍵暗号化／復号化部２０７は、指定実行器用ソフト鍵Ｅ（Ｘ，ＫＡ）をプレーヤＸに固有の秘密情報ＳＸで復号化し、ソフト鍵ＫＡを得る（ステップＳ１０７）。なお、このとき、指定プレーヤ用ソフト鍵Ｅ（Ｘ，ＫＡ）がプレーヤＸ用でないならば、ソフト鍵ＫＡが復号できずソフトウェアは実行できない。

【００４２】次に、ソフト鍵暗号化／復号化部２０７は、復号化されたソフト鍵ＫＡを、暗号化ソフトウェア復号部２０９に入力する。また、実行制御部２０５は、接続部２０１を介して、ディスクの暗号化ソフトウェア記録部８から暗号化ソフトウェアＥ（ＫＡ，ｓｏｆｔＡ）を読み出し、暗号化ソフトウェア復号部２０９に入力する。応じて、暗号化ソフトウェア復号部２０９は、ソフト鍵暗号化／復号化部２０７から入力されたソフト鍵ＫＡを用いて、ソフトウェアｓｏｆｔＡを復号化する（ステップＳ１０８）。次に、暗号化ソフトウェア復号部２０９は、その復号化されたソフトウェアｓｏｆｔＡをソフトウェア実行部２１０に入力する。従って、ソフトウェア実行部２１０は、復号化されたソフトウェアを実行する（ステップＳ１０９）。

【００４３】一方、前述のステップＳ１０２における検

索の結果、入力されたソフトウェア固有情報ＩＤＡと一致する実行不可ソフトウェア固有情報ＩＤＡ'が記憶部２０３に記憶されていない場合、ソフトウェアＩＤ検索部２０２は、実行制御部２０５にソフト実行許可の情報を入力する（ステップＳ１０６）。以下、ステップＳ１０７～Ｓ１０９の処理は、前述のステップＳ１０７～Ｓ１０９の動作と全く同じである。

【００４４】（ｂ）指定実行器の変更手続き

次に、図３を参照して、指定実行器の変更手続きについて説明する。なお、以下の説明では、現在ブレーヤＸでしか実行できないディスク１に格納されているソフトウェアをブレーヤＸでは実行不可とし、ブレーヤＸと異なる他のブレーヤＹで実行できるようにする指定実行器変更手続きについて述べる。

【００４５】まず、変更先をブレーヤＹにするという情報（実行器識別子）が、図示しないキーボード，マウス等の入力装置から実行器指定部２１１に入力される（ステップＳ２０１）。すると、実行器指定部２１１は、接続部２０１を介して、情報記録部１２から指定実行器用ソフト鍵Ｅ（Ｘ，ＫＡ）を読み出し、ソフト鍵暗号化／復号化部２０７に入力する。また、実行器指定部２１１は、秘密情報格納部２０８からブレーヤＸに固有の秘密情報ＳＸを読み出し、ソフト鍵暗号化／復号化部２０７に入力する。ソフト鍵暗号化／復号化部２０７は、秘密情報格納部２０８から入力されるブレーヤＸに固有の秘密情報ＳＸを用いて、指定実行器用ソフト鍵Ｅ（Ｘ，ＫＡ）をソフト鍵ＫＡに復号化し、その後、実行器指定部２１１から与えられる変更先ブレーヤＹの実行器識別子からブレーヤＹ用の公開鍵を生成し、この生成した公開鍵を用いてソフト鍵ＫＡを暗号化し、ブレーヤＹ用ソフト鍵Ｅ（Ｙ，ＫＡ）を得る（ステップＳ２０２）。また、実行器指定部２１１は、先に情報記録部１２に記録されているブレーヤＸ用ソフト鍵Ｅ（Ｘ，ＫＡ）を、接続部２０１を介して消去する。さらに、実行器指定部２１１は、接続部２０１を介して、情報記録部１２に、ブレーヤＹ用ソフト鍵Ｅ（Ｙ，ＫＡ）を指定実行器用ソフト鍵として記録する。このブレーヤＹ用ソフト鍵Ｅ（Ｙ，ＫＡ）は、ブレーヤＹに固有の秘密情報ＳＹ（ブレーヤＹの秘密情報部２０８に格納されている）のみによってしか復号化できない。したがって、以後このディスク１は、ブレーヤＹでしか実行できなくなる。

【００４６】次に、実行器指定部２１１は、接続部２０１を介して、情報記録部１２に記録されているソフトウェア識別子の累積数ＣＮＴ［Ａ］の値が１だけ増えるように記録を更新する（ステップＳ２０３）。次に、実行器指定部２１１は、更新された新しい累積数ＣＮＴ［Ａ］の値を新しいソフトウェア識別子の基準数ＮＵＭ［Ａ］の値とし、実行不可ソフトウェア固有情報ＩＤＡ'と対にしてソフトウェア識別子として、実行不可ソフトウェア情報更新部２１２を介して、記憶部２０３に

書き込む（ステップＳ２０４）。このとき、実行器指定部２１１は、同時に記憶部２０３から古い基準数の値を消去する。これによって、このディスク１に格納されているソフトウェアは、以後、ブレーヤＸでは実行できなくなる。

【００４７】次に、実行器指定部２１１は、接続部２０１を介して、情報記録部１２からソフトウェア識別子であるソフトウェア固有情報ＩＤＡと累積数ＣＮＴ［Ａ］とを読み出し、また秘密情報格納部２０８からブレーヤＸに固有の秘密情報ＳＸを読み出し、それぞれ署名情報作成部２１３に入力する。署名情報作成部２１３は、入力されたソフトウェア識別子であるソフトウェア固有情報ＩＤＡと累積数ＣＮＴ［Ａ］に対して、ブレーヤＸに固有の秘密情報ＳＸを用いてブレーヤＸでしか作成できない署名情報を作成し、この作成された署名情報を接続部２０１を介して新たな署名情報として情報記録部１２に記録する（ステップＳ２０５）。このとき、署名情報作成部２１３は、同時に古い署名情報を消去する。

【００４８】なお、上記指定ブレーヤ変更手続き前にブレーヤＸ用のディスクをコピーしておいても、指定ブレーヤ変更手続き後には、記憶部２０３での基準数ＮＵＭ［Ａ］が、このコピーされたディスクの累積数よりも大きくなるので、図２のステップＳ１０５におけるブレーヤ内の基準数ＮＵＭ［Ａ］とディスク内の累積数ＣＮＴ［Ａ］との比較動作で実行不可と判断され、ブレーヤＸで不所望にコピーディスクが実行されることを防止できる。

【００４９】以上説明したように、第１の実施例によれば、ソフト鍵を指定実行器以外では復号できないようなソフトウェア保護システムにおいて、指定実行器の変更を可能とし、不正なコピーを防止しつつ、ソフトウェアを任意の実行器で実行できる環境を実現することができる。

【００５０】なお、上記第１の実施例は、ソフトウェア本体をそのソフトウェアの全ディスクに共通のソフト鍵ＫＡで暗号化し、そのソフト鍵ＫＡを指定された実行器でしか復号できないように暗号化するシステムとして構成されているが、本発明は、ソフトウェア自身を指定した実行可能実行器でしか復号できないように暗号化するように構成されてもよく、この場合も第１の実施例と同様な効果が得られる。

【００５１】また、上記第１の実施例では、ソフトウェアを指定実行器以外で実行されないようにするためにソフト鍵を用いたが、ディスクに指定実行器のＩＤ情報を格納しておき、実行器側ではいつもソフトウェアの実行を行う前に、ディスクのＩＤ情報が自装置に対応するＩＤ情報かをチェックし、自装置に対応するＩＤ情報の場合のみソフトウェアを実行するようにしてもよい。

【００５２】また、上記第１の実施例では、ディスク１を譲渡する際に、無効ディスクを示す情報として、順序

付けられた数を有する累積数および基準数を用いたが、これら累積数および基準数に代えて乱数を発生し、情報記録部１２および記憶部２０３には、この乱数をソフトウェア固有情報と対にしてソフトウェア識別子として記録しておくようにしてもよい。この場合、記憶部２０３には発生した乱数が全て消去せずに記録され、情報記録部１２には新しい乱数が発生する毎に古い乱数が新しい乱数に書き換えられる。そして、ディスク１上のソフトウェア識別子を記憶部２０３に記憶されている全てのソフトウェア識別子と比較し、一致するものがない場合にのみソフトウェアの実行を許可することになる。

【００５３】また、上記第１の実施例では、ディスク１上のソフトウェア識別子の正当性を確保するため、これを対象としたディジタル署名を生成したが、ディジタル署名の対象をソフトウェア識別子と指定実行器用ソフト鍵と暗号化ソフトウェアの内容の全部または一部を対象としてもよい。これによって、暗号化ソフトウェア記録部１１に記録されている暗号化ソフトウェアの内容および実行器識別子の正当性も確保することができる。

【００５４】また、上記第１の実施例では、ディスク１上のデータの正当性を示すためにディジタル署名を使用しているが、ソフトウェア識別子などを指定実行器以外では復号できない形で暗号化してもよく、この場合も上記第１の実施例と同様な効果が得られる。

【００５５】また、上記第１の実施例では、ソフトウェア識別子のソフトウェアを識別する情報として、ソフトウェア種別毎に異なり、かつディスク毎には共通のソフトウェア固有情報ＩＤＡを用いたが、これに代えて各ディスクに固有の識別子を用いてもよい。これによって、ディスク１の指定実行器変更手続き後に、先のディスクと同じ種別のソフトウェアを格納する別のディスクを実行しようとするときにも対処できる。

【００５６】また、上記第１の実施例では、オフラインのソフトウェア流通形態を想定しているが、この発明をオンラインのソフトウェア流通形態に適用しても、上記第１の実施例と同様な効果が得られる。

【００５７】（２）第２の実施例

本発明の第２の実施例は、第１の実施例で述べたソフトウェア保護システムを用いたレンタルソフトウェアシステムとして構成されている。図４は、この第２の実施例のレンタルソフトウェアシステムにおける処理手順を示すフローチャートである。以下、第１の実施例で述べた構成を援用しつつ、図４を参照して、第２の実施例の詳細を説明する。

【００５８】このレンタルソフトシステムでは、レンタル専用のディスクを導入する。第１の実施例では、ディスク１の情報記録部１２（図１参照）には、ソフト鍵に関する情報として、暗号化された指定実行器用ソフト鍵のみが記録されている。これに対し、第２の実施例におけるレンタル専用ディスクでは、ディスク内の情報記録部１２に、指定実行器用ソフト鍵だけではなく、レンタル店用ソフト鍵が常に記録されている。情報記録部１２におけるその他の情報は、第１の実施例において情報記録部１２に記録されている情報と同じである。

【００５９】レンタル店Ｘで会員Ｙ（プレーヤＹと同じものと考える）に、上記レンタル専用ディスクを貸す場合の手続きを述べる。レンタル店Ｘでは、会員Ｙを変更先として第１の実施例で述べたように変更手続きをレンタル店のプレーヤで行なう。このとき、このディスク１内の指定実行器用ソフト鍵が、会員Ｙのプレーヤでしか実行できない形式に暗号化されている（ステップＳ３０１）。会員Ｙは、自分自身のプレーヤＹに、このディスク１を差し込み、ソフトウェアを実行させる（ステップＳ３０２）。以下、このディスク１内のソフトウェアが実行される手順は、第１の実施例で述べた通りである。

【００６０】次に、会員Ｙがディスクをレンタル店Ｘに返却する場合について述べる。会員Ｙは、第１の実施例で述べた指定実行器変更手続きで、譲渡先としてレンタル店を指定するのではなく、単に返却手続きをすればよい。なぜならば、ディスク１の情報記録部１２には、常にレンタル店用ソフト鍵が記録されているため、レンタル店Ｘでは、このレンタル店用ソフト鍵を用いて、ディスク１の実行が可能であるためである。このとき、会員Ｙのプレーヤにおける実行器指定部２１１は、情報記録部１２のプレーヤＹ用ソフト鍵を消去し、累積数を１増やし、記憶部２０３の基準数の更新を行なう（ステップＳ３０３）。この処理によって、レンタル用ディスクをコピーしておいて返却手続き後に実行しようとしても、図２のステップＳ１０５によってそのコピーディスクは実行できない。すなわち、レンタル専用ディスクでは、会員Ｙ用のソフト鍵の消去はできるが、指定実行器の変更手続きは、レンタル店でのみ可能である。

【００６１】上記のように第２の実施例によれば、レンタル先用に暗号化されたレンタルソフトウェアをレンタル店に返却するときに、会員側ではレンタル店を指定実行器として指定実行器の変更手続きを行う必要がなく、面倒な手間が省ける。また、レンタル専用ディスクは指定実行器でしか実行できないため、レンタルソフトウェアのまた貸しも防げる。さらに、累積数と基準数との更新により、会員が不正なコピーを作成するのも防げる。また、レンタル専用ディスクの指定実行器の変更手続きが可能なのはレンタル店のみであるから、会員間の貸し借りもできない。

【００６２】（３）第３の実施例

図５は、本発明の第３の実施例の構成を示すブロック図である。図５において、この第３の実施例では、指定された回数だけコピーができるマスターディスク１０を用いる。このマスターディスク１０には、図１のディスク１に記録されている情報に加えて、コピー可能回数Ｎｏ

［ｃｏｐｙ］，累計数ＳＵＭ［ｄｉｓｋ］およびマスターディスク識別子が情報記録部１２に記録されている。マスターディスク１０のその他の記録情報は、図１のディスク１の記録情報と同様である。

【００６３】プレーヤ２には、第１の実施例で述べたプレーヤ２の構成に加えて、コピー制御部２１４およびバッファメモリ２１５が追加されている。図６は、この第３の実施例のソフトウェア保護システムにおける処理手順を示すフローチャートである。以下、この図６を参照して、第３の実施例の動作を説明する。

【００６４】まず、マスターディスク１０からコピーディスクを作成する場合について説明する。なお、マスターディスク１０は、プレーヤＸでのみ実行できるものとする。マスターディスク１０が接続部２０１に接続されると（ステップＳ４０１）、コピー制御部２１４は、情報記録部１２からマスターディスク識別子を読み出し、接続されたディスクがマスターディスク１０であることを識別する（ステップＳ４０２）。次に、コピー制御部２１４は、情報記録部１２から累計数ＳＵＭ［ｄｉｓｋ］を読み出し、マスターディスク１０からのコピーが最初か否かを判断する（ステップＳ４０３）。マスターディスク１０から１度もコピーディスクが作成されていない場合（すなわち、累計数ＳＵＭ［ｄｉｓｋ］が０の場合）、コピー制御部２１４は、実行不可ソフトウェア情報更新部２１２は、接続部２０１を介して、情報記録部１２からコピー可能回数Ｎｏ［ｃｏｐｙ］および累計数ＳＵＭ［ｄｉｓｋ］を読み出し、記憶部２０３に、それぞれ、Ｎｏ［ｃｏｐｙ，Ｘ］およびＳＵＭ［Ｘ］として格納する（ステップＳ４０４）。また、コピー制御部２１４は、接続部２０１を介して、情報記録部１２からマスターディスク識別子を読み出し、上記コピー可能回数Ｎｏ［ｃｏｐｙ，Ｘ］および累計数ＳＵＭ［Ｘ］と対にして、記憶部２０３に格納する。

【００６５】一方、マスターディスク１０から少なくとも１度はコピーディスクが作成されている場合、コピー制御部２１４は、記憶部２０３に記憶されているコピー可能回数Ｎｏ［ｃｏｐｙ，Ｘ］および累計数ＳＵＭ［Ｘ］と、情報記録部１２に記録されているコピー可能回数Ｎｏ［ｃｏｐｙ］および累計数ＳＵＭ［ｄｉｓｋ］とを比較し、両者が等しいか否かを確認する（ステップＳ４０５）。ステップＳ４０５において両者の不一致が確認された場合、コピー制御部２１４は、マスターディスク１０からのコピーが不許可であると判断する（ステップＳ４０６）。したがって、この場合、マスターディスク１０のコピーは行われない。一方、ステップＳ４０５において両者の一致が確認された場合、コピー制御部２１４は、情報記録部１２に記録されたコピー可能回数Ｎｏ［ｃｏｐｙ］と、記憶部２０３に記憶された累計数ＳＵＭ［Ｘ］との大小関係を比較し、不等式Ｎｏ［ｃｏｐｙ］＞ＳＵＭ［Ｘ］が成り立つ場合にのみ、マスターディスク１０からのコピーを許可する（ステップＳ４０７）。

【００６６】次に、マスターディスク１０のコピー許可が出て、別のディスクにマスタディスクの内容をコピーする場合の動作について説明する。連続して１度にコピーをする回数ｎが、外部の入力装置（図示せず）からコピー制御部２１４に対して入力されると、コピー制御部２１４は、接続部２０１を介して、情報記録部１２に記録されている累計数ＳＵＭ［ｄｉｓｋ］を指定されたコピー回数ｎだけ増加するように更新し、同様に、記憶部２０３内の累計数ＳＵＭ［Ｘ］を更新する（ステップＳ４０８）。ただし、このｎは、更新される累計数が、コピー可能回数Ｎｏ［ｃｏｐｙ］と等しくまたは大きくならないような値に選ばれる。次に、コピー制御部２１４は、接続部２０１を介して、マスターディスク１０から暗号化ソフトウェアおよび指定実行器用ソフト鍵を読み出し、バッファメモリ２１４に格納する（ステップＳ４０９）。

【００６７】コピーディスクは、第１の実施例で述べたディスクと同じ記録形式で、情報記録部１２と暗号化ソフトウェア記録部８とを含む。このコピーディスクがマスターディスク１０と差し替えられて接続部２０１に接続されると（ステップＳ４１０）、図示しない外部の入力装置から実行器指定部２１１に、指定実行器に関する情報が入力される（ステップＳ４１１）。この実行器指定情報は、コピー制御部２１１に入力される。応じて、コピー制御部２１４は、バッファメモリ２１５から暗号化ソフトウェアを読み出し、接続部２０１を介して、コピーディスクの暗号化ソフトウェア記録部１１に書き込む（ステップＳ４１２）。また、コピー制御部２１４は、コピーディスクの情報記録部１２に、ソフトウェア識別子として、ソフトウェア固有情報と累積数を記録する（ステップＳ４１２）。このとき、累積数は０で記録される。さらに、コピー制御部２１４は、指定実行器用ソフト鍵および署名情報を、それぞれ、ソフト鍵暗号化／復号化部２０７および証明情報作成部２１３によって作成させ、接続部２０１を介してコピーディスクの情報記録部１２に記録させる（ステップＳ４１２）。これで、新しいコピーディスクが１つ生成されたことになる。その後、コピー制御部２１４は、予め指定されたコピー回数ｎだけのコピーディスクを生成する。ｎ個のコピーディスクが生成されると、コピー制御部２１４は、バッファメモリ２１５に格納されている暗号化ソフトウェアを消去する（ステップＳ４１３）。

【００６８】以上のように、上記第３の実施例によれば、新たにある指定された特定の実行器でしか実行できないコピーディスクを、予め指定された回数だけ生成することができる。

【００６９】

【発明の効果】請求項１の発明によれば、ソフトウェア

を実行させるべき実行器に固有の第２の固有情報を記録媒体に格納しておき、実行器では、記録媒体からソフトウェアおよび第２の固有情報を読み出し、当該第２の固有情報が自装置に固有の情報である場合のみ、当該ソフトウェアの実行を受け付けるようにしているので、指定された実行器以外でソフトウェアが実行されるのを防止することができる。また、実行器の変更先が指定されると、記録媒体に格納された第２の固有情報を、指定された他の実行器に固有の情報に変換するようにしているので、ソフトウェアを実行可能な実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納された第１の固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されている第１の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしているので、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【００７０】請求項２の発明によれば、実行器の変更先が指定されたとき、記録媒体に格納された累積数および実行不可情報記憶手段に記憶された基準数のそれぞれに所定値を加算しておき、その後、実行不可情報記憶手段に記憶されている第１の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、累積数が基準数よりも大きい場合は、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。そのため、変更先の実行器において再び元の実行器が変更先として指定された場合であっても、元の実行器でのソフトウェアの実行が可能となる。

【００７１】請求項３の発明によれば、実行器の変更先が指定されたとき、実行器で乱数を発生し、この乱数を実行不可情報記憶手段に追加して書き込むと共に、記録媒体に格納された乱数を当該乱数で書き換え、その後、実行不可情報記憶手段に記憶されている第１の固有情報と同一の固有情報を有する記録媒体が元の実行器に装着されたとしても、記録媒体に格納されている乱数と同一の乱数が実行不可情報記憶手段に記憶されていない場合は、当該記録媒体に格納されているソフトウェアの実行を許可するようにしている。そのため、変更先の実行器において再び元の実行器が変更先として指定された場合であっても、元の実行器でのソフトウェアの実行が可能となる。

【００７２】請求項４の発明によれば、暗号化されたソフト鍵を記録媒体に格納しておき、実行器では、このソフト鍵を固有の秘密情報を用いて復号化し、さらに復号化されたソフト鍵を用いて、記録媒体から読み出したソフトウェアを復号化し実行するようにしているので、指定された実行器以外でソフトウェアが実行されるのを防止することができる。また、実行器の変更先が指定されると、復号化されたソフト鍵を、指定された他の実行器でのみ復号可能なように暗号化し、記録媒体に格納された暗号化されたソフト鍵を、このとき暗号化されたソフト鍵に書き換えるようにしているので、ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納されたソフトウェア固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されているソフトウェア固有情報と同一のソフトウェア固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしているので、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正に実行されるのを防止することができる。

【００７３】請求項５の発明によれば、暗号化されたソフトウェア，ソフトウェア固有情報，暗号化されたソフト鍵および累積数の内、少なくともいずれか１つを対象として作成されたディジタル署名情報を記録媒体に格納しておき、実行器では、記録媒体に格納されているディジタル署名情報が正当か否かを確認し、正当でない場合は、当該記録媒体に格納されているソフトウェアの実行を受け付けないようにしているので、記録媒体の格納情報の正当性をより正確に確認でき、不正な複製品を防止できる。

【００７４】請求項６の発明によれば、記録媒体がコピーされる毎に更新される累計数を実行器に記憶しておき、記録媒体に格納されたコピー可能回数が当該累計数よりも大きい場合のみ、当該記録媒体のコピーを許可するようにしているので、記録媒体のコピー回数を予め定められた回数に制限することができる。

【００７５】請求項７の発明によれば、貸し主側の実行器は、記録媒体に格納された第１のソフト鍵を用いてソフトウェアの復号化を行うので、借り主側の実行器では、記録媒体を貸し主に返却するとき、記録媒体中の第２のソフト鍵を書き換える必要がない。

【００７６】請求項８の発明によれば、記録媒体に格納されたソフトウェア自体が指定実行器でのみ復号可能なように暗号化されているので、指定された実行器以外でソフトウェアが実行されるのを防止することができる。また、実行器の変更先が指定されると、復号化されたソフトウェアを、指定された他の実行器でのみ復号可能なように暗号化し、記録媒体に格納されたソフトウェアを、このとき暗号化されたソフトウェアに書き換えるようにしているので、ソフトウェアを実行する実行器をユーザ側で容易に変更することができる。また、実行器の変更先が指定されると、記録媒体に格納されたソフトウェア固有情報を、実行不可情報記憶手段に書き込んでおき、その後、実行不可情報記憶手段に記憶されているソフトウェア固有情報と同一のソフトウェア固有情報を有する記録媒体が元の実行器に装着されても、当該記録媒

体に格納されているソフトウェアの実行を受け付けないようにしているので、実行器の変更指定前にコピーされたソフトウェアが、元の実行器で不正にに実行されるのを防止できる。

【図面の簡単な説明】

【図１】本発明の第１の実施例に係るソフトウェア保護システムの構成を示すブロック図である。

【図２】本発明の第１の実施例のソフトウェア保護システムにおけるソフトウェア実行動作の処理手順を示すフローチャートである。

【図３】本発明の第１の実施例のソフトウェア保護システムにおける指定実行器の変更手続きの処理手順を示すフローチャートである。

【図４】本発明の第２の実施例のレンタルソフトウェアシステムにおける処理手順を示すフローチャートである。

【図５】本発明の第３の実施例の構成を示すブロック図である。

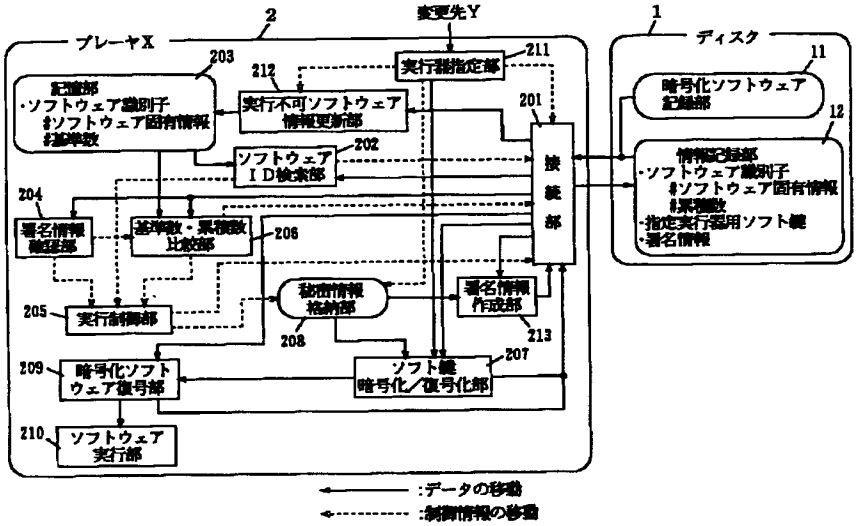
【図６】本発明の第３の実施例のソフトウェア保護システムにおける処理手順を示すフローチャートである。

【図７】従来のソフトウェア保護システムの構成を示す＊ブロック図である。

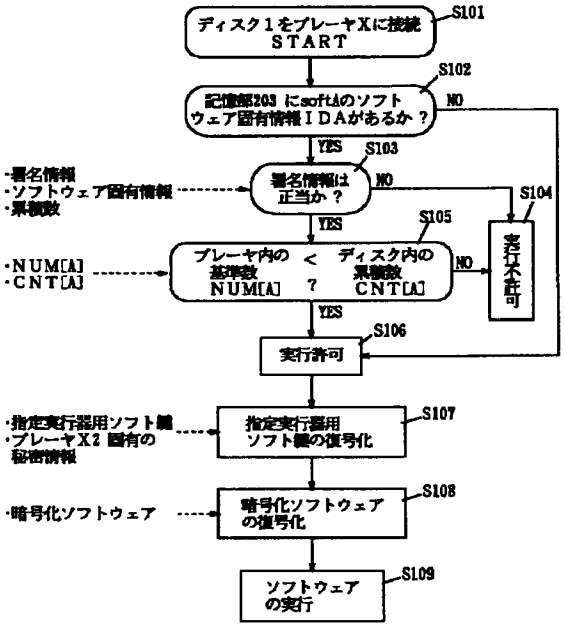
【符号の説明】

１…ディスク
１１…暗号化ソフトウェア記録部
１２…情報記録部
２…プレーヤ
２０１…接続部
２０２…ソフトウェアＩＤ検索部
２０３…記憶部
２０４…署名情報確認部
２０５…実行制御部
２０６…基準数・累積数比較部
２０７…ソフト鍵暗号化／復号化部
２０８…秘密情報格納部
２０９…暗号化ソフトウェア復号部
２１０…ソフトウェア実行部
２１１…実行器指定部
２１２…実行不可ソフトウェア情報更新部
２１３…署名情報作成部
２１４…コピー制御部

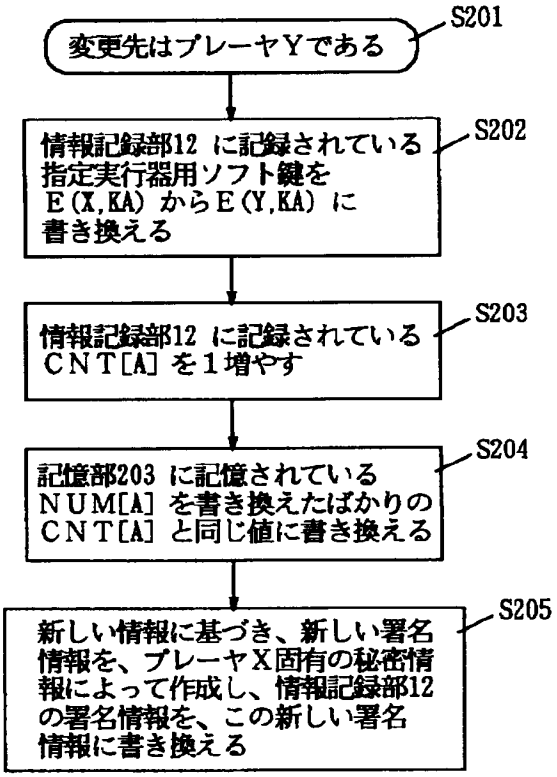
【図１】



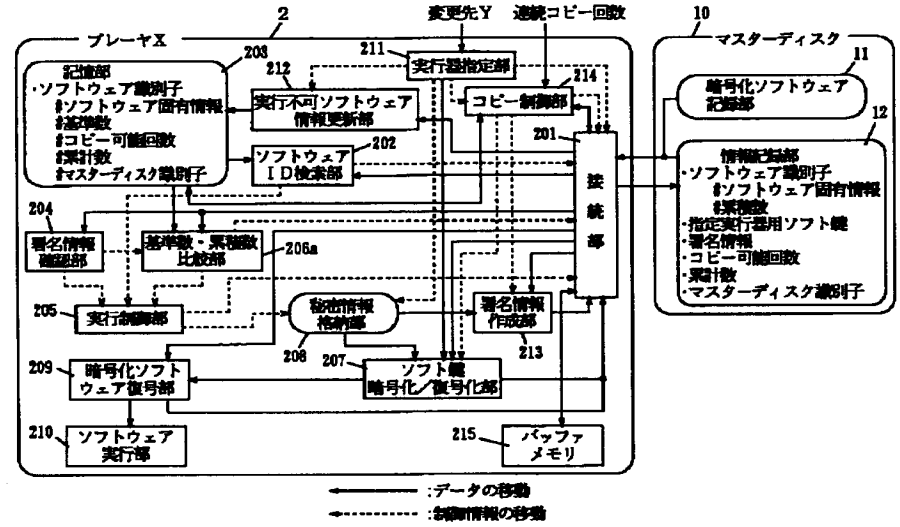
【図２】


ディスク１をプレーヤXに接続
START
S101
記憶部203 にsoftAのソフトウェア固有情報ＩＤAがあるか？
S102
NO
YES
S103
署名情報は正当か？
NO
S104
YES
S105
プレーヤ内の基準数 NUM[A] ＜ ディスク内の累積数 CNT[A] ？
NO
実行不許可
YES
S106
実行許可
・署名情報
・ソフトウェア固有情報
・累積数
・NUM[A]
・CNT[A]
・指定実行器用ソフト鍵
・プレーヤX2 固有の秘密情報
指定実行器用ソフト鍵の復号化
S107
・暗号化ソフトウェア
暗号化ソフトウェアの復号化
S108
ソフトウェアの実行
S109

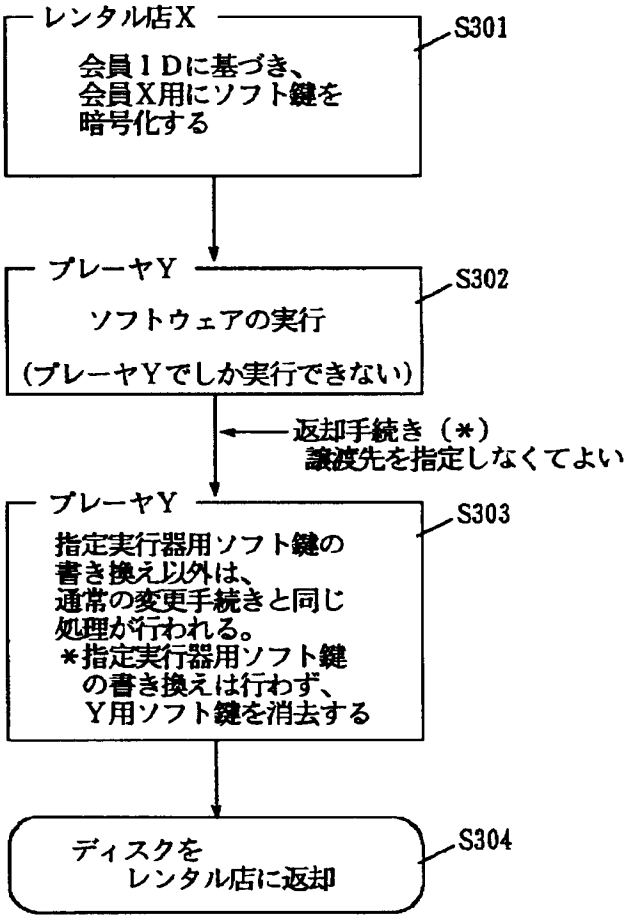
【図３】


変更先はプレーヤＹである
S201
情報記録部12 に記録されている指定実行器用ソフト鍵をＥ(X,KA) からＥ(Y,KA) に書き換える
S202
情報記録部12 に記録されているＣＮＴ[A] を１増やす
S203
記憶部203 に記憶されているＮＵＭ[A] を書き換えたばかりのＣＮＴ[A] と同じ値に書き換える
S204
新しい情報に基づき、新しい署名情報を、プレーヤＸ固有の秘密情報によって作成し、情報記録部12の署名情報を、この新しい署名情報に書き換える
S205

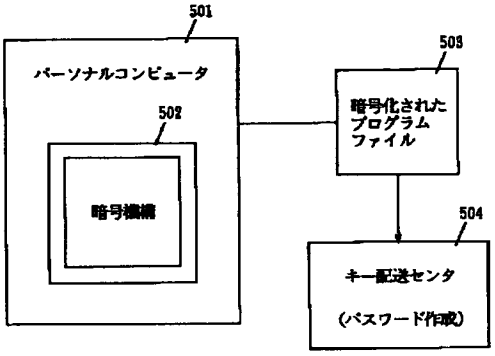
【図５】


プレーヤX
2
変更先Y
連続コピー回数
マスターディスク
10
記憶部
・ソフトウェア識別子
#ソフトウェア固有情報
#基準数
#コピー可能回数
#累計数
#マスターディスク識別子
203
実行器指定部
211
実行不可ソフトウェア情報更新部
212
コピー制御部
214
ソフトウェアＩＤ検査部
202
接続部
201
暗号化ソフトウェア記録部
11
情報記録部
・ソフトウェア識別子
#ソフトウェア固有情報
#累積数
・指定実行器用ソフト鍵
・署名情報
・コピー可能回数
・累計数
・マスターディスク識別子
12
署名情報確認部
204
基準数・累積数比較部
206a
実行制御部
205
秘密情報格納部
208
署名情報作成部
213
207
ソフト鍵暗号化／復号化部
暗号化ソフトウェア復号部
209
ソフトウェア実行部
210
バッファメモリ
215
:データの移動
:制御情報の移動

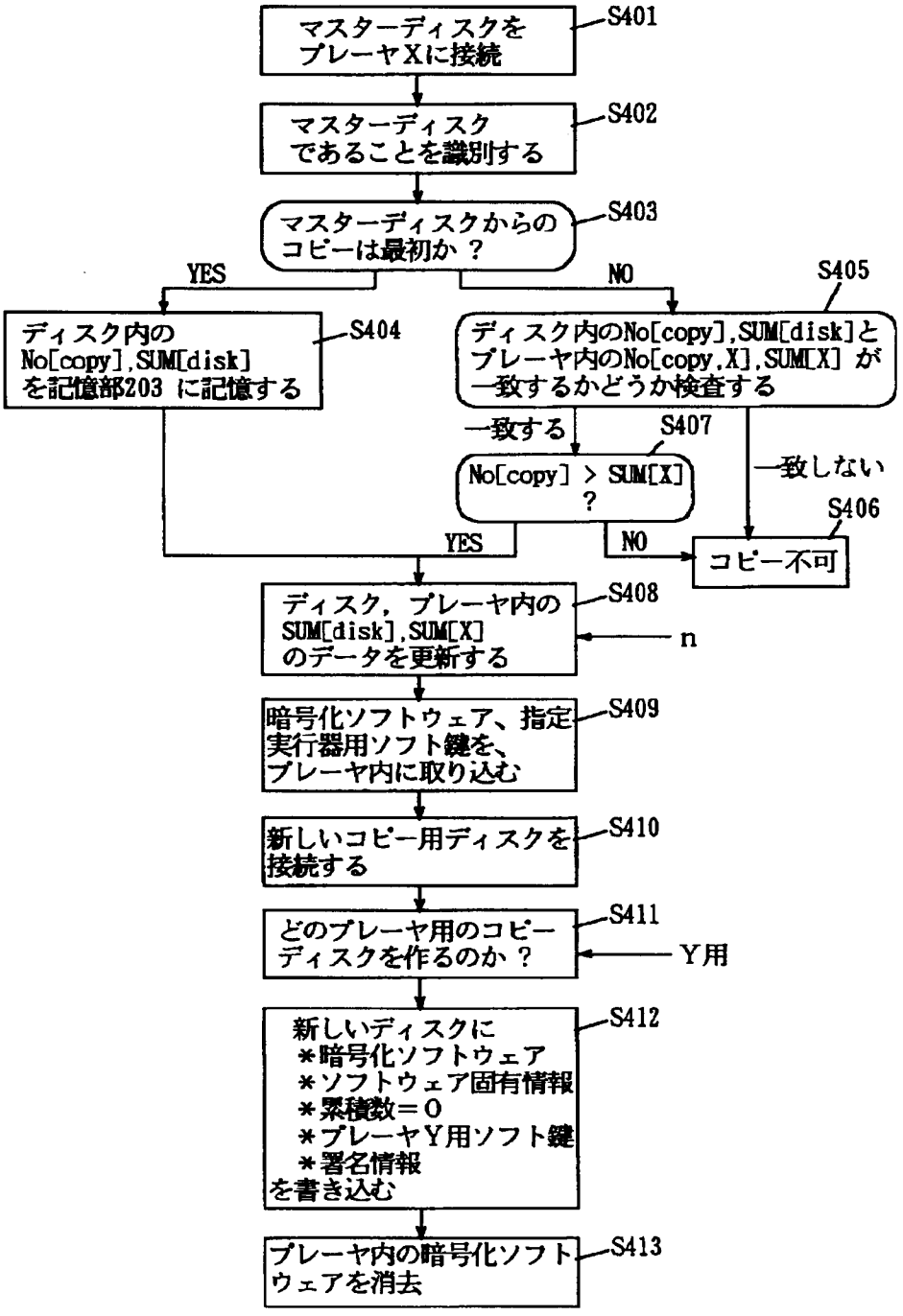
【図４】


レンタル店X
会員１Ｄに基づき、
会員X用にソフト鍵を
暗号化する
S301
プレーヤY
ソフトウェアの実行
(プレーヤYでしか実行できない)
S302
返却手続き（＊）
譲渡先を指定しなくてよい
プレーヤY
指定実行器用ソフト鍵の
書き換え以外は、
通常の変更手続きと同じ
処理が行われる。
＊指定実行器用ソフト鍵
の書き換えは行わず、
Y用ソフト鍵を消去する
S303
ディスクを
レンタル店に返却
S304

【図７】


501
パーソナルコンピュータ
502
暗号機構
503
暗号化された
プログラム
ファイル
504
キー配送センタ
(パスワード作成)

【図６】


マスターディスクを
プレーヤXに接続
S401
マスターディスク
であることを識別する
S402
マスターディスクからの
コピーは最初か？
S403
YES
NO
S405
ディスク内の
No[copy],SUM[disk]
を記憶部203 に記憶する
S404
ディスク内のNo[copy],SUM[disk]と
プレーヤ内のNo[copy,X],SUM[X] が
一致するかどうか検査する
一致する
S407
No[copy] > SUM[X]
？
一致しない
S406
YES
NO
コピー不可
ディスク，プレーヤ内の
SUM[disk],SUM[X]
のデータを更新する
S408
n
暗号化ソフトウェア、指定
実行器用ソフト鍵を、
プレーヤ内に取り込む
S409
新しいコピー用ディスクを
接続する
S410
どのプレーヤ用のコピー
ディスクを作るのか？
S411
Y用
新しいディスクに
＊暗号化ソフトウェア
＊ソフトウェア固有情報
＊累積数＝０
＊プレーヤY用ソフト鍵
＊署名情報
を書き込む
S412
プレーヤ内の暗号化ソフト
ウェアを消去
S413

フロントページの続き

(72)発明者　宮地　充子
大阪府門真市大字門真1006番地　松下電器
産業株式会社内